(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－332745
(P2000－332745A)
(43)公開日　平成12年11月30日(2000.11.30)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ	9/00	６４１　５Ｃ０６４
Ｈ０４Ｈ　1/00		Ｈ０４Ｈ	1/00	Ｆ　５Ｊ１０４
Ｈ０４Ｊ　3/00		Ｈ０４Ｊ	3/00	Ｍ　５Ｋ０２８
				Ｂ　５Ｋ０３０
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ	11/20	１０２Ｚ

審査請求　未請求　請求項の数10　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願平11－140340

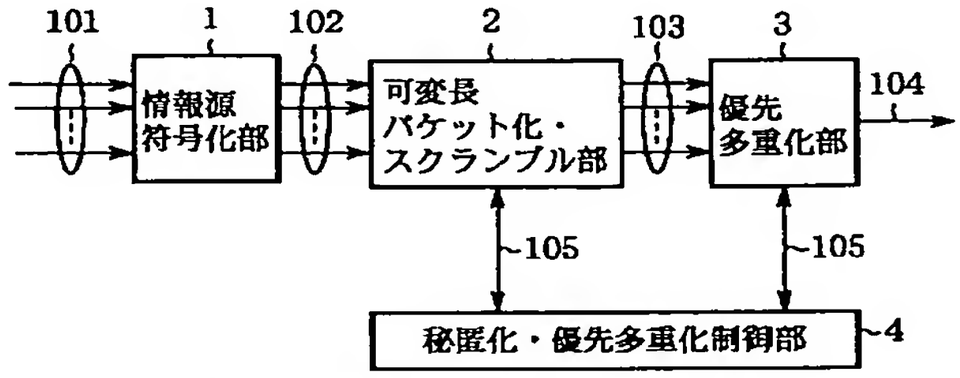
(22)出願日　平成11年５月20日(1999.5.20)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　松崎　一博
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　加藤　嘉明
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100066474
弁理士　田澤　博昭　（外１名）

最終頁に続く

(54)【発明の名称】　限定受信方式の送信装置および受信装置

(57)【要約】
【課題】　多重化遅延時間に比較してスクランブル鍵の更新周期が比較的小さい場合には、古い鍵でスクランブルされたバケットと新しい鍵でスクランブルされたバケットとが混在して、受信側で復号不能になるという課題があった。
【解決手段】　情報源符号化部１と、可変長バケット化・スクランブル部２と、優先多重化部３と、秘匿化・優先多重化制御部４とを有する限定受信方式の送信装置において、秘匿化・優先多重化制御部４が、多重化ビット列１０４において最大多重化遅延時間よりも大きな時間間隔でスクランブル鍵を更新するように制御する。



1：情報源符号化部（情報源符号化手段）
2：可変長パケット化・スクランブル部
（パケット化・スクランブル手段）
3：優先多重化部（優先多重化手段）
4：秘匿化・優先多重化制御部（秘匿化・優先多重化制御手段）
101：コンテンツ
102：情報源符号化ビット列
103：可変長パケット列（パケット列）
104：多重化ビット列

【特許請求の範囲】

【請求項１】　各種のコンテンツを符号化する情報源符号化手段と、
該情報源符号化手段から出力される情報源符号化ビット列をパケットに格納するとともに該パケットの一部分を秘匿化してパケット列を生成するパケット化・スクランブル手段と、
複数の情報源符号化ビット列を該情報源符号化ビット列毎に与えられた多重化遅延に基づく優先度に基づいてパケット単位に多重化して多重化ビット列を生成する優先多重化手段と、
前記パケット化・スクランブル手段および前記優先多重化手段を制御する秘匿化・優先多重化制御手段とを有する限定受信方式の送信装置において、
前記秘匿化・優先多重化制御手段が、前記多重化ビット列において、最大多重化遅延時間よりも大きな時間間隔でスクランブル鍵を更新するように制御することを特徴とする限定受信方式の送信装置。

【請求項２】　パケット化・スクランブル手段が、情報源符号化ビット列を可変長パケットのペイロードに格納して可変長パケットを生成することを特徴とする請求項１記載の限定受信方式の送信装置。

【請求項３】　各種のコンテンツを符号化する情報源符号化手段と、
該情報源符号化手段から出力される情報源符号化ビット列をパケットに格納するとともに該パケットの一部分を秘匿化してパケット列を生成するパケット化・スクランブル手段と、
複数の情報源符号化ビット列を該情報源符号化ビット列毎に与えられた多重化遅延に基づく優先度に基づいてパケット単位に多重化して多重化ビット列を生成する優先多重化手段と、
前記パケット化・スクランブル手段および前記優先多重化手段を制御する秘匿化・優先多重化制御手段とを有する限定受信方式の送信装置において、
前記パケット化・スクランブル手段が、パケットの一部分を秘匿化するために使用したスクランブル鍵を格納するＥＣＭを特定するためのＥＣＭ特定番号をパケットのヘッダに登録することを特徴とする限定受信方式の送信装置。

【請求項４】　パケット化・スクランブル手段が、情報源符号化ビット列を可変長パケットのペイロードに格納して可変長パケットを生成することを特徴とする請求項３記載の限定受信方式の送信装置。

【請求項５】　パケット単位に多重化遅延に基づく優先度に応じて多重化された多重化ビット列をコンテンツ毎のパケット列に分離する優先多重分離手段と、
パケット列において秘匿化された部分の秘匿を解除するとともに、パケットを分解して情報源符号化ビット列を生成するパケット分解・デスクランブル手段と、

情報源符号化ビット列を復号してコンテンツを再生する情報源復号手段とを有する限定受信方式の受信装置において、
前記パケット分解・デスクランブル手段が、ＥＣＭ特定番号を参照して、パケットの一部分を秘匿化するために使用したスクランブル鍵を特定し、パケットの秘匿化部分の秘匿を解除することを特徴とする限定受信方式の受信装置。

【請求項６】　各種のコンテンツを符号化する情報源符号化手段と、
該情報源符号化手段から出力される情報源符号化ビット列をパケットに格納して該パケットの一部分を秘匿化するパケット化・スクランブル手段と、
複数の情報源符号化ビット列を該情報源符号化ビット列毎に与えられた多重化遅延に基づく優先度に基づいてパケット単位に多重化して多重化ビット列を生成する優先多重化手段と、
前記パケット化・スクランブル手段および前記優先多重化手段を制御する秘匿化・優先多重化制御手段とを有する限定受信方式の送信装置において、
前記秘匿化・優先多重化制御手段が、秘匿化についての優先度に基づいてパケットの秘匿特性を制御することを特徴とする限定受信方式の送信装置。

【請求項７】　秘匿化・優先多重化制御手段は、コンテンツ毎の情報源符号化モード単位に設定された秘匿化についての優先度に基づいてパケットの秘匿特性を制御することを特徴とする請求項６記載の限定受信方式の送信装置。

【請求項８】　秘匿化・優先多重化制御手段は、秘匿化についての優先度に基づき、暗号の種類、およびＣＢＣモードやＯＦＢモード等の暗号の利用モードを変えて暗号化することを特徴とする請求項６または請求項７に記載の限定受信方式の送信装置。

【請求項９】　秘匿化・優先多重化制御手段は、秘匿化についての優先度に基づき、秘匿化期間を制御することを特徴とする請求項６または請求項７に記載の限定受信方式の送信装置。

【請求項１０】　パケット化・スクランブル手段が、情報源符号化ビット列を可変長パケットのペイロードに格納して可変長パケットを生成することを特徴とする請求項６から請求項９のいずれか１項に記載の限定受信方式の送信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、デジタル化された映像信号、音響信号、その他データ等のマルチメディアデータを符号化および多重化して伝送する際に、信号をスクランブルして秘匿化し、予め契約を結んだ特定の受信者のみがスクランブル信号を復号できる限定受信方式の送信装置および受信装置に関するものである。

【０００２】

【従来の技術】図１０は、例えば片方善治監修「マルチメディア産業応用技術体系」ｐｐ．４９５～４９６、フジ・テクノシステム（１９９７年）に示された従来の限定受信方式の送信装置の構成を示すブロック図である。また、図１１は、同様に上記文献に示された従来の限定受信方式の受信装置の構成を示すブロック図である。

【０００３】図１０において、２１は情報源符号化部、２２は固定長パケット化・スクランブル部、２３は多重化部、２４は秘匿化・多重化制御部である。また、４０１は映像信号、音声信号、種々のデータ等のコンテンツ、４０２は情報源符号化ビット列、４０３は固定長パケット列、４０４は多重化ビット列、４０５は秘匿化・多重化のための制御信号である。なお、図において矢印はそれぞれのコンテンツまたは符号化処理されたビットストリームの伝送路を示し、情報源符号化部２１等では、複数の伝送路により伝送される複数のコンテンツまたはビットストリームが並列に処理される。図１１において、２５は多重分離部、２６は固定長パケット分解・デスクランブル部、２７は情報源復号部である。

【０００４】次に動作について説明する。まず、従来の限定受信方式の送信装置における処理について図１０を参照して説明する。情報源符号化部２１は、映像信号、音声信号、データ等の複数のコンテンツ４０１に対して情報源符号化処理を行なって情報源符号化ビット列４０２を生成する。固定長パケット化・スクランブル部２２は、それぞれの情報源符号化ビット列４０２を適切に分割して固定長パケットのペイロードに格納して固定長パケットを生成するとともに、固定長パケットのペイロードをスクランブル処理して秘匿化し固定長パケット列４０３を生成する。さらに、固定長パケット化・スクランブル部２２は、コンテンツに対する情報源符号化ビット列４０２をペイロードに格納した通常の固定長パケットに加えて、スクランブル鍵などの秘匿化情報をＥＣＭ（Entitlement Control Message ）として固定長パケットに格納して出力する。多重化部２３は、固定長パケット列４０３を固定長パケット単位に多重化して多重化ビット列４０４を生成する。また、秘匿化・多重化制御部２４は、秘匿に使用するスクランブル鍵の更新タイミング、ＥＣＭの多重化タイミング等を制御する。

【０００５】次に、従来の限定受信方式の受信装置における処理について図１１を参照して説明する。従来の限定受信方式の受信装置における処理は、送信装置における処理と逆の処理となる。図１１に示されるように、多重分離部２５は多重化ビット列４０４をコンテンツ毎に分離して、それぞれのコンテンツに対応した複数の固定長パケット列４０３を生成する。固定長パケット分解・デスクランブル部２６は、ＥＣＭとして送られてきた秘＊

＊匿化情報を用いて固定長パケット列４０３の秘匿状態を解除するとともに、パケットを分解して情報源符号化ビット列４０２を生成する。情報源復号部２７は、情報源符号化ビット列４０２を復号して、映像信号、音声信号、種々のデータ等のコンテンツ４０１を再生する。

【０００６】さらに、従来の限定受信方式における伝送信号の多重方式、及び秘匿化・多重化制御部２４の動作について説明する。図１２は、例えば電波産業界標準規格「ＢＳデジタル放送の送信・運用条件（ＡＲＩＢ　ＳＴＤ－Ｂ２０　１．０版）」ｐｐ．２０～３８（１９９８年１１月６日）に示された従来の限定受信方式における伝送信号の多重方式を説明する図である。なお、多重化に関して、送信装置における処理と受信装置における処理とは逆の処理となるので、ここでは送信装置における処理について説明する。

【０００７】コンテンツ毎（情報源毎）のそれぞれの情報源符号化ビット列４０２を固定長のパケットに分割し、パケットのペイロードに対してスクランブル処理を施し、スクランブルされた固定長パケットをパケット単位に多重化して多重化ビット列４０４を生成する。スクランブル鍵等の秘匿化情報は、ＥＣＭとして固定長パケットに格納して多重化する。ＥＣＭは、コンテンツ毎に指定することも、複数コンテンツに共通なものとして指定することも可能である。また、ＥＣＭは周期的（時間間隔：ｔ）に送出される。１つのＥＣＭにより、それぞれ奇数鍵（odd key ）および偶数鍵（even key）と呼ばれて区別される２種類のスクランブル鍵が同時に運ばれる。ＥＣＭに格納された奇数鍵と偶数鍵とは同時には更新されずに、１つずつ順番に更新される。

【０００８】秘匿化するか否かについての秘匿化／非秘匿化情報、秘匿化に使用したスクランブル鍵の種別（奇数鍵／偶数鍵）情報は、固定長パケット単位に付加することが可能である。これら秘匿化に関する情報は、固定長パケットのヘッダに格納される。

【０００９】秘匿化に関する設定内容が更新されたＥＣＭを格納するパケットの直後に、更新した鍵を使用してスクランブル処理を実施したパケットを多重化して伝送した場合には、受信側では更新された鍵の取り込みが間に合わずにデスクランブルエラーが生じることがある。そのために、内容更新のあったＥＣＭを格納するパケットと、更新した鍵でスクランブルされたパケットとは、通常、受信側における鍵取り込み時間を考慮して時間間隔を開けて多重化される。例えば、更新したスクランブル鍵をＥＣＭで送る時刻をＴｅｃｍ、更新したスクランブル鍵の受信側での使用時刻をＴｓ、スクランブル鍵の更新周期をＴｔ、多重化遅延を考慮しない転送時間を含めた受信側における鍵の取り込み時間を△Ｔとすると、

$$Ts - 2Tt - \Delta T \leq Tecm < Ts - \Delta T \quad （式１）$$

受信側において奇数鍵または偶数鍵の使用が有効な期間

として与えられるものである。すなわち、送信側では、更新周期Ｔｔごとに奇数鍵から偶数鍵へまたは偶数鍵から奇数鍵へスクランブル鍵が更新されて、更新されたスクランブル鍵を基にしてスクランブル処理がなされる。しかし、奇数鍵から次の奇数鍵への更新または偶数鍵から次の偶数鍵への更新は２Ｔｔを周期として実施され、また各バケットには使用されるスクランブル鍵の種別（奇数鍵または偶数鍵）が登録されているから、受信側におけるスクランブル鍵の使用有効期間は２Ｔｔとなる。そして、秘匿化・多重化制御部２４は、式１を満足するように、スクランブル鍵の更新周期、ＥＣＭの更新タイミング等を制御する。

【００１０】

【発明が解決しようとする課題】従来の限定受信方式の送信装置等は以上のように構成されているので、情報源符号化ビット列を分割して固定長バケットのペイロードに格納する際に、バケットを固定長にするためにダミーバイトを挿入する必要があり、多重化の効率が低下するという課題があった。

【００１１】また、従来の限定受信方式の送信装置等では、多重化に関して優先度が付された情報源符号化ビット列を秘匿化して多重化伝送する場合、優先度の低いバケットの多重化遅延時間に比較してスクランブル鍵の更新周期Ｔｔが比較的小さい場合には、受信側では古い鍵でスクランブルされたバケットと新しい鍵でスクランブルされたバケットとが混在して届くために復号不能になるという課題があった。

【００１２】また、従来の限定受信方式の送信装置等では、コンテンツ毎の情報源符号化モードに応じて秘匿化の優先度を設定することはなかったので、それぞれの情報源符号化モードに応じて柔軟な秘匿特性を設定することができないという課題があった。ここで、秘匿特性とは、コンテンツを秘匿化する期間設定、秘匿化に用いられる暗号の種類、及びＣＢＣ（Cipher Block Chaining）モードやＯＦＢ（Output Feed Back）モード等の暗号の利用モード等の秘匿化に関する属性全般を指すものである。また、情報源符号化モードとは、各コンテンツを符号化する際の符号化方式を示すものであり、ＭＰＥＧ－２ビデオ規格を例にとれば、イントラ予測モード、前方向予測モードおよび両方向予測モードが符号化モードとして与えられている。

【００１３】この発明は上記のような課題を解決するためになされたもので、複数の情報源符号化ビット列をバケットに格納するとともに秘匿化して多重化伝送する際に、多重化の効率を向上させた限定受信方式の送信装置および受信装置を得ることを目的とする。

【００１４】また、この発明は、新しい鍵でスクランブルされたバケットと古い鍵でスクランブルされたバケットとの混在等による復号不能を防止して、信頼性の高い限定受信方式の送信装置および受信装置を得ることを目的とする。

【００１５】さらに、この発明は、コンテンツ毎の情報源符号化モードに応じて柔軟な秘匿特性を設定できる限定受信方式の送信装置および受信装置を得ることを目的とする。

【００１６】

【課題を解決するための手段】この発明に係る限定受信方式の送信装置は、秘匿化・優先多重化制御手段が多重化ビット列において、最大多重化遅延時間よりも大きな時間間隔でスクランブル鍵を更新するように制御するものである。

【００１７】この発明に係る限定受信方式の送信装置は、バケット化・スクランブル手段が情報源符号化ビット列を可変長バケットのペイロードに格納して可変長バケットを生成するようにしたものである。

【００１８】この発明に係る限定受信方式の送信装置は、バケット化・スクランブル手段がバケットの一部分を秘匿化するために使用したスクランブル鍵を格納するＥＣＭを特定するためのＥＣＭ特定番号をバケットのヘッダに登録するようにしたものである。

【００１９】この発明に係る限定受信方式の受信装置は、バケット分解・デスクランブル手段が、ＥＣＭ特定番号を参照して、バケットの一部分を秘匿化するために使用したスクランブル鍵を特定し、バケットの秘匿化部分の秘匿を解除するようにしたものである。

【００２０】この発明に係る限定受信方式の送信装置は、秘匿化・優先多重化制御手段が秘匿化についての優先度に基づいてバケットの秘匿特性を制御するようにしたものである。

【００２１】この発明に係る限定受信方式の送信装置は、秘匿化・優先多重化制御手段がコンテンツ毎の情報源符号化モード単位に設定された秘匿化についての優先度に基づいてバケットの秘匿特性を制御するようにしたものである。

【００２２】この発明に係る限定受信方式の送信装置は、秘匿化・優先多重化制御手段が秘匿化についての優先度に基づき、暗号の種類、およびＣＢＣモードやＯＦＢモード等の暗号の利用モードを変えて暗号化するようにしたものである。

【００２３】この発明に係る限定受信方式の送信装置は、秘匿化・優先多重化制御手段が秘匿化についての優先度に基づき秘匿化期間を制御するようにしたものである。

【００２４】

【発明の実施の形態】以下、この発明の実施の一形態を説明する。

実施の形態１．図１は、この発明の実施の形態１による限定受信方式の送信装置の構成を示すブロック図である。また、図２は、この発明の実施の形態１による限定受信方式の受信装置の構成を示すブロック図である。

【００２５】図１において、１は各種コンテンツ情報に対して符号化処理を行なう情報源符号化部（情報源符号化手段）、２は可変長パケット化および秘匿化を実施する可変長パケット化・スクランブル部（パケット化・スクランブル手段）、３は優先度に応じて多重化を実施する優先多重化部（優先多重化手段）、４は可変長パケット化・スクランブル部２および優先多重化部３を制御する秘匿化・優先多重化制御部（秘匿化・優先多重化制御手段）である。また、１０１は映像信号、音声信号、種々のデータ等のコンテンツ、１０２は情報源符号化ビット列、１０３は可変長パケット列（パケット列）、１０４は多重化ビット列、１０５は秘匿化・優先多重化のための制御信号である。

【００２６】図２において、５は多重化ビット列１０４をコンテンツ毎に可変長パケット列１０３に分離する優先多重分離部（優先多重分離手段）、６は秘匿を解除するとともに可変長パケットを分解して情報源符号化ビット列１０２を生成する可変長パケット分解・デスクランブル部（パケット分解・デスクランブル手段）、７は情報源符号化ビット列１０２を復号してコンテンツ１０１を再生する情報源復号部（情報源復号手段）である。

【００２７】次に動作について説明する。第１に、この発明の実施の形態１による限定受信方式の送信装置における処理について図１を参照して説明する。情報源符号化部１は、映像信号、音声信号、データ等の複数のコンテンツ１０１に対して情報源符号化処理を行なって情報源符号化ビット列１０２を生成する。この符号化処理を実施するに際して、映像信号の情報源符号化についてはＭＰＥＧ－２ビデオ規格に準拠しており、映像フレーム、映像フィールド等に相当する「ピクチャ」と呼ばれる符号化ユニットを単位として、イントラ予測モード、前方向予測モード、両方向予測モードの中から情報源符号化モードが選択される。一方、音声信号、種々のデータ等に関しては、所定の時間長や所定のバイト長を符号化ユニットとして情報源符号化処理が実施される。

【００２８】次に、可変長パケット化・スクランブル部２は、それぞれの情報源符号化ビット列１０２を符号化ユニット毎に分割して可変長パケットのペイロードに格納して可変長パケットを生成するとともに、可変長パケットのペイロードをスクランブル処理して秘匿化し可変長パケット列１０３を生成する。

【００２９】図３は、この発明の実施の形態１により使用される可変長パケットの構成を示す図である。２０１は可変長パケットの先頭を識別するためのユニークワードが格納されたパケットスタートコード、２０２はパケットに格納されるコンテンツ毎に異なる番号が付与されるパケット識別子、２０３は秘匿化／非秘匿化情報、秘匿化に使用する奇数鍵／偶数鍵の区別情報、ＣＢＣやＯＦＢ等の暗号の利用モード等を通知する秘匿化情報、２０４は当該可変長パケットの秘匿化に係るＥＣＭを格納

する可変長パケットのパケット識別子の値を通知するＥＣＭ識別番号、２０５は可変長パケットのペイロード長を示すペイロード長、２０６は可変長パケットのヘッダ部分の誤りチェック、およびスクランブル処理を行なった際のパケットスタートコード２０１とのエミュレーションを防止するために付与されたＣＲＣ、２０７は符号化されたビット列を格納する可変長パケットペイロードである。なお、コンテンツまたは情報源符号化モード等に応じて種別の異なる複数のＥＣＭが用意されており、ＥＣＭ識別番号２０４により、当該パケットに係るコンテンツまたは情報源符号化モードに応じたＥＣＭの種別が識別される。

【００３０】秘匿化の際には、秘匿化・優先多重化制御部４から出力される制御信号１０５により、コンテンツ内容に応じて、あるいは符号化ユニット毎の情報源符号化モードに応じて、秘匿化に使用する暗号の種類、ＣＢＣやＯＦＢ等の暗号の利用モード、秘匿化／非秘匿化情報等が可変長パケット毎に制御されて、これら制御情報がそれぞれの可変長パケットの秘匿化情報２０３のフィールドに書き込まれる。

【００３１】例えば、映像コンテンツの場合、秘匿化・優先多重化制御部４は、秘匿化について符号化ユニットの情報源符号化モードに対して規定される以下のような優先度Ｐｃａに基づき、次のように制御する。

Ｐｃａ＝１　：　全ての符号化ユニットを秘匿化。

Ｐｃａ＝２　：　イントラ予測モード以外の符号化ユニットを秘匿化。

Ｐｃａ＝３　：　両方向予測モードの符号化ユニットのみ秘匿化。

Ｐｃａ＝４　：　秘匿化なし。

【００３２】また、音声コンテンツや種々のデータコンテンツに対する秘匿化については、秘匿化・優先多重化制御部４は、秘匿化の優先度に応じて、秘匿化期間または非秘匿化期間を符号化ユニット単位に制御する。また、秘匿化の優先度によっては、使用する暗号の種類を変えたり、ＣＢＣモードやＯＦＢモード等の暗号の利用モードを変えることによって秘匿の強度を制御する。なお、秘匿化に関して個々の可変長パケットの秘匿化情報２０３のフィールドに収容されないスクランブル鍵等の秘匿化関連情報は、ＥＣＭとして可変長パケットのペイロードに格納して送られる。

【００３３】次に、優先多重化部３は、コンテンツ毎の可変長パケット列１０３を優先多重化して、固定ビットレート（ＣＢＲ）の多重化ビット列１０４を生成する。この際、優先多重化時の多重化特性は、各コンテンツに与えられた多重化遅延に関する優先度に基づいて制御信号１０５により制御される。多重化遅延に関する優先度は、ＥＣＭおよび制御情報を最優先とする。また、リアルタイム伝送が必要なコンテンツに対する優先度を高くするとともに、リアルタイム伝送を必要とはしないコン

テンツに対する優先度を低くする。さらに、映像と当該映像に付随する音声との場合のように、同期再生が必要となる複数のコンテンツには同じ優先度を与える。

【００３４】また、秘匿化・優先多重化制御部４は、既に述べた可変長パケット毎の秘匿化優先度の制御に加えて、秘匿に使用するスクランブル鍵の更新タイミングの制御、ＥＣＭの多重化タイミングの制御、各コンテンツに与えられた多重化遅延に関する優先度に基づく優先多重化制御等を行なう制御信号１０５を出力する。

【００３５】第２に、この発明の実施の形態１による限定受信方式の受信装置における処理について図２を参照して説明する。図２に示されるように、優先多重分離部５は、パケットスタートコード２０１、パケット識別子２０２、ペイロード長２０５、およびＣＲＣ２０６を参照して、多重化ビット列１０４をコンテンツ毎に分離して可変長パケット列１０３を生成する。

【００３６】次に、可変長パケット分解・デスクランブル部６は、秘匿化情報２０３とＥＣＭ識別番号２０４により同定されたＥＣＭとを参照して可変長パケットのペイロードの秘匿を解除するとともに、可変長パケットを分解してコンテンツ毎の情報源符号化ビット列１０２を生成する。そして、情報源復号部７は、情報源符号化ビット列１０２を復号して映像信号、音声信号、種々のデータ等のコンテンツ１０１を再生する。

【００３７】第３に、この発明の実施の形態１による限定受信方式における伝送信号の多重方式、及び秘匿化・優先多重化制御部４の動作について説明する。図４は、この発明の実施の形態１による限定受信方式における伝送信号の多重方式を説明する図である。なお、多重化に関して、送信側の処理と受信側の処理とは逆の処理となるので、ここでは送信側の処理に基づいて説明する。

【００３８】コンテンツ毎の（情報源毎）のそれぞれの＊

$$Tt > Tdmx$$

を満足するように、スクランブル鍵の更新周期Ｔｔを制御する。

【００４２】既に述べたように、送信側において奇数鍵から偶数鍵へまたは偶数鍵から奇数鍵へスクランブル鍵が更新される周期はＴｔであるが、受信側における奇数鍵または偶数鍵の使用有効期間は２Ｔｔであるので、例え送信側で更新直前のスクランブル鍵によりスクランブルされたパケットが多重化遅延により受信側に遅れて到着したとしても、その遅延時間がＴｔ以内であれば受信側でデスクランブル処理が可能であるから、式１および式２を満たすように制御することで、古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが受信側で混在することが防止される。

【００４３】Ｔｄｍｘに関しては、優先多重化シミュレーション等によって見積もった値を使用してもよいし、多重化遅延に関する閾値制御を行なって各パケットの多重化遅延がＴｄｍｘを超えないようにしてもよい。

＊情報源符号化ビット列１０２を符号化ユニット毎に可変長のパケットに格納し、パケットのペイロードに対してスクランブル処理を施し、コンテンツ毎に与えられた多重化遅延に関する優先度に基づいてスクランブル処理された可変長パケットをパケット単位に多重化して多重化ビット列１０４を生成する。スクランブル鍵等の秘匿化情報は、ＥＣＭとして可変長パケットに格納して多重化する。

【００３９】この発明の実施の形態１による限定受信方式では、ＥＣＭはコンテンツ毎に指定することも、複数コンテンツに共通なものとして指定することも可能である。また、ＥＣＭは周期的（時間間隔：ｔ）に送出される。１つのＥＣＭにより、それぞれ奇数鍵および偶数鍵と呼ばれて区別される２種類のスクランブル鍵が同時に運ばれる。ＥＣＭに格納された奇数鍵と偶数鍵とは同時には更新されずに、１つずつ順番に更新される。

【００４０】秘匿化／非秘匿化情報、秘匿化に使用したスクランブル鍵の種別（奇数鍵／偶数鍵）情報は、可変長パケット単位に付加することが可能である。これら秘匿化に関する情報は、可変長パケットのヘッダに秘匿化情報２０３として格納される。

【００４１】この発明の実施の形態１による限定受信方式では、多重化遅延に関する優先多重化を行なうために、パケットが生成されてから多重化されるまでの遅延時間（多重化遅延）がコンテンツ毎に異なる。それゆえ、受信側では古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが混在するのを防止する必要があるが、式１を満足するように秘匿化・優先多重化制御部４においてスクランブル鍵の更新周期やＥＣＭの更新タイミングを制御するのみではデスクランブルエラーが生じ得る。そこで、多重化されるビット列の最大多重化遅延Ｔｄｍｘを考慮して、

（式２）

【００４４】以上のように、この発明の実施の形態１によれば、各コンテンツ毎の情報源符号化ビット列１０２を可変長パケット化した後に多重化して多重化ビット列１０４を生成するようにしたので、パケットを可変長に形成することができて固定長パケットのようにダミーバイトを挿入する必要がないから、多重化の効率を向上することができるという効果を奏する。

【００４５】また、多重化されるビット列の最大多重化遅延時間よりもスクランブル鍵の更新周期を大きくとることで、受信側において古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが混在するのが防止されるから、符号化ビット列の復号を確実に実施できて、限定受信方式における信頼性を高めることができるという効果を奏する。

【００４６】また、秘匿化・優先多重化制御部４により、コンテンツに応じて、あるいはコンテンツ毎の情報源符号化モードに応じて秘匿化の優先度を設定する構成

とすることで、コンテンツあるいはコンテンツ毎の情報源符号化モードに応じた柔軟な秘匿特性を設定できるから、伝送するコンテンツの内容や用途に応じた柔軟な秘匿機能を実現できるという効果を奏する。

【００４７】また、秘匿化・優先多重化制御部４が秘匿化についての優先度に基づき、暗号の種類および暗号の利用モードを変えて暗号化するように構成したので、コンテンツの内容または情報源符号化モード等に応じて秘匿の強度を適応的に制御することができるという効果を奏する。

【００４８】さらに、秘匿化・優先多重化制御部４が秘匿化についての優先度に基づき、秘匿化期間を制御するように構成したので、コンテンツの内容または情報源符号化モード等に応じて、一定の期間中、契約者のみ復号可能にすること、あるいは受信者すべてに復号可能にすること等を選別して実施することができるから、受信形態を柔軟に設定することができるという効果を奏する。

【００４９】実施の形態２．この発明の実施の形態２による限定受信方式の送信装置および受信装置は、実施の形態１による限定受信方式の送信装置および受信装置と基本的には同じ構造を有しており、その送信装置の構成は同様に図１により示され、また受信装置の構成は同様に図２により示される。実施の形態２は、実施の形態１と比較すると、可変長パケットの構成が異なる点でのみ相違する。

【００５０】図５は、この発明の実施の形態２により使用される可変長パケットの構成を示す図である。図３に示される実施の形態１により使用される可変長パケットと比較すると、ＥＣＭバージョン番号２０８を有する点で相違している。ＥＣＭバージョン番号（ＥＣＭ特定番号）２０８は、ＥＣＭ識別番号（ＥＣＭ特定番号）２０４で識別されるそれぞれの種別のＥＣＭについて、所定の秘匿化特性を付与されて個別化された個々のＥＣＭを特定するためのバージョン番号として与えられるものであり、それぞれの種別のＥＣＭにおいて内容の更新が生じた場合には、ＥＣＭバージョン番号が１ずつ増分される。

【００５１】次に、動作について説明する。基本的な動作については実施の形態１と同様であるので、ここでは実施の形態１と相違する点について説明する。第１に、秘匿化の際には、秘匿化・優先多重化制御部４から出力される制御信号１０５により、実施の形態１と同様に適用されたスクランブル処理に係るＥＣＭの種別を識別するための番号がＥＣＭ識別番号２０４のフィールドに書き込まれ、さらにこの実施の形態２ではスクランブル処理に使用されたスクランブル鍵が格納された個別のＥＣＭを特定するためのバージョン番号がＥＣＭバージョン番号２０８のフィールドに書き込まれる。

【００５２】第２に、秘匿化解除の際には、可変長パケット分解・デスクランブル部６は、ＥＣＭ識別番号２０４およびＥＣＭバージョン番号２０８により特定されるＥＣＭと、秘匿化情報２０３とを参照して、当該可変長パケットのスクランブル処理に使用されたスクランブル鍵を特定することにより、可変長パケットのペイロードの秘匿を解除する。

【００５３】以上のように、この発明の実施の形態２によれば、実施の形態１と同様に多重化の効率の向上、柔軟な秘匿機能の実現という効果を奏するとともに、各可変長パケットがＥＣＭバージョン番号を格納するフィールドをヘッダに備えることで、当該可変長パケットのスクランブル処理に使用されたスクランブル鍵を特定することができるので、古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが受信側で混在しても符号化ビット列の復号を確実に実施できて、限定受信方式における信頼性を高めることができるという効果を奏する。

【００５４】実施の形態３

図６は、この発明の実施の形態３による限定受信方式の送信装置の構成を示すブロック図である。また、図７は、この発明の実施の形態３による限定受信方式の受信装置の構成を示すブロック図である。図６において、図１と同一符号は同一または相当部分を示すのでその説明を省略する。また、図７において、図２と同一符号は同一または相当部分を示すのでその説明を省略する。実施の形態３は、実施の形態１と比較すると、符号化ユニットを固定長パケットに格納して多重化する点で相違する。

【００５５】図６において、１０は固定長パケット化および秘匿化を実施する固定長パケット化・スクランブル部（パケット化・スクランブル手段）、１０６は固定長パケット列（パケット列）である。また、図７において、１１は秘匿を解除するとともに固定長パケットを分解して情報源符号化ビット列１０２を生成する固定長パケット分解・デスクランブル部（パケット分解・デスクランブル手段）である。

【００５６】次に動作について説明する。第１に、この発明の実施の形態３による限定受信方式の送信装置における処理について説明する。なお、情報源符号化部１、優先多重化部３、および秘匿化・優先多重化制御部４の動作は実施の形態１におけるのと同様であるので、その説明を省略する。

【００５７】固定長パケット化・スクランブル部１０は、それぞれの情報源符号化ビット列１０２を符号化ユニット毎に分割して固定長パケットのペイロードに格納し固定長パケットを生成するとともに、固定長パケットのペイロードをスクランブル処理して秘匿化し固定長パケット列１０６を生成する。情報源符号化ビット列１０２を固定長パケットのペイロードに格納する際には、図１２に示すように情報源符号化ユニットの先頭部が常に固定長パケットのペイロードの先頭部に一致するように

処理がなされる。このために、固定長バケットのペイロードにはダミーバイトが挿入される。

【００５８】図８は、この発明の実施の形態３により使用される固定長バケットの構成を示す図である。３０１は固定長バケットの先頭を示すバケットスタートコード、３０２はバケットに格納されるコンテンツ毎に異なる番号が付与されるバケット識別子、３０３は秘匿化／非秘匿化情報、秘匿化に使用する奇数鍵／偶数鍵の区別情報、ＣＢＣやＯＦＢ等の暗号の利用モード等を通知する秘匿化情報、３０４は当該固定長バケットの秘匿化に係るＥＣＭを格納する固定長バケットのバケット識別子の値を通知するＥＣＭ識別番号、３０５は固定長バケットのペイロードに格納されたコンテンツとダミーバイトとを区別するための有効バイト長、３０７は符号化されたコンテンツを格納する固定長バケットペイロードである。

【００５９】なお、秘匿化に関して個々の固定長バケットの秘匿化情報３０３のフィールドに収容されないスクランブル鍵等の秘匿化関連情報は、ＥＣＭとして固定長バケットのペイロードに格納して送られる。

【００６０】第２に、この発明の実施の形態３による限定受信方式の受信装置における処理について図７を参照して説明する。図７に示されるように、優先多重分離部５は、バケットスタートコード３０１、バケット識別子３０２、および有効バイト長３０５を参照して、多重化ビット列１０４をコンテンツ毎に分離して固定長バケット列１０６を生成する。

【００６１】次に、固定長バケット分解・デスクランブル部１１は、秘匿化情報３０３とＥＣＭ識別情報３０４により同定されたＥＣＭとを参照して固定長バケットのペイロードの秘匿を解除するとともに、固定長バケットを分解してコンテンツ毎の情報源符号化ビット列１０２を生成する。そして、情報源復号部７は情報源符号化ビット列１０２を復号して映像信号、音声信号、種々のデータ等のコンテンツ１０１を再生する。

【００６２】なお、この発明の実施の形態３による限定受信方式における伝送信号の多重方式、及び秘匿化・優先多重化制御部４の動作については、実施の形態１と同様であるのでその説明を省略する。

【００６３】以上のように、この発明の実施の形態３によれば、多重化されるビット列の最大多重化遅延時間よりもスクランブル鍵の更新周期を大きくとることで、受信側において古い鍵でスクランブルされたバケットと新しい鍵でスクランブルされたバケットとが混在するのが防止されるので、符号化ビット列の復号を確実に実施できて、限定受信方式における信頼性を高めることができるという効果を奏する。

【００６４】さらに、秘匿化・優先多重化制御部４により、コンテンツに応じて、あるいはコンテンツ毎の情報源符号化モードに応じて秘匿化の優先度を設定する構成

とすることで、コンテンツあるいはコンテンツ毎の情報源符号化モードに応じた柔軟な秘匿特性を設定できるから、伝送するコンテンツの内容や用途に応じた柔軟な秘匿機能を実現できるという効果を奏する。

【００６５】実施の形態４．この発明の実施の形態４による限定受信方式の送信装置および受信装置は、実施の形態３による限定受信方式の送信装置および受信装置と基本的には同じ構造を有しており、その送信装置の構成は同様に図６により示され、また受信装置の構成は同様に図７により示される。実施の形態４は、実施の形態３と比較すると、固定長バケットの構成が異なる点でのみ相違する。

【００６６】図９は、この発明の実施の形態４により使用される固定長バケットの構成を示す図である。図８に示される実施の形態３により使用される固定長バケットと比較すると、ＥＣＭバージョン番号３０８を有する点で相違している。ＥＣＭバージョン番号３０８は、ＥＣＭ識別番号３０４で識別されるそれぞれの種別のＥＣＭについて、所定の秘匿化特性を付与されて個別化された個々のＥＣＭを特定するためのバージョン番号として与えられるものであり、それぞれの種別のＥＣＭにおいて内容の更新が生じた場合には、ＥＣＭバージョン番号が１ずつ増分される。

【００６７】次に、動作について説明する。基本的な動作については実施の形態３と同様であるので、ここでは実施の形態３と相違する点について説明する。第１に、秘匿化の際には、秘匿化・優先多重化制御部４から出力される制御信号１０５により、実施の形態３と同様に、適用されたスクランブル処理に係るＥＣＭの種別を識別するための番号がＥＣＭ識別番号３０４のフィールドに書き込まれ、さらにこの実施の形態４ではスクランブル処理に使用されたスクランブル鍵が格納された個別のＥＣＭを特定するためのバージョン番号がＥＣＭバージョン番号３０８のフィールドに書き込まれる。

【００６８】第２に、秘匿化解除の際には、固定長バケット分解・デスクランブル部１１は、ＥＣＭ識別番号３０４およびＥＣＭバージョン番号３０８により特定されるＥＣＭと、秘匿化情報３０３とを参照して、当該固定長バケットのスクランブル処理に使用されたスクランブル鍵を特定することにより、固定長バケットのペイロードの秘匿を解除する。

【００６９】以上のように、この発明の実施の形態４によれば、実施の形態３と同様に多重化の効率の向上、柔軟な秘匿機能の実現という効果を奏するとともに、各固定長バケットがＥＣＭバージョン番号を格納するフィールドをヘッダに備えることで、当該固定長バケットのスクランブル処理に使用されたスクランブル鍵を特定することができるので、古い鍵でスクランブルされたバケットと新しい鍵でスクランブルされたバケットとが受信側で混在しても符号化ビット列の復号を確実に実施でき

て、限定受信方式における信頼性を高めることができるという効果を奏する。

【００７０】

【発明の効果】以上のように、この発明によれば、秘匿化・優先多重化制御手段が多重化ビット列において最大多重化遅延時間よりも大きな時間間隔でスクランブル鍵を更新するように制御する構成としたので、受信側において古い鍵でスクランブルされたバケットと新しい鍵でスクランブルされたバケットとが混在するのが防止されるから、符号化ビット列の復号を確実に実施できて、限定受信方式における信頼性を高めることができるという効果を奏する。

【００７１】この発明によれば、バケット化・スクランブル手段が情報源符号化ビット列を可変長バケットのペイロードに格納して可変長バケットを生成するように構成したので、固定長バケットのようにダミーバイトを挿入する必要がなく多重化の効率を向上することができるという効果を奏する。

【００７２】この発明によれば、バケット化・スクランブル手段がバケットの一部分を秘匿化するために使用したスクランブル鍵を格納するＥＣＭを特定するためのＥＣＭ特定番号をバケットのヘッダに登録するように構成したので、当該バケットのスクランブル処理に使用されたスクランブル鍵を特定することができるから、古い鍵でスクランブルされたバケットと新しい鍵でスクランブルされたバケットとが受信側で混在しても符号化ビット列の復号を確実に実施できて、限定受信方式における信頼性を高めることができるという効果を奏する。

【００７３】この発明によれば、バケット分解・デスクランブル手段が、ＥＣＭ特定番号を参照して、バケットの一部分を秘匿化するために使用したスクランブル鍵を特定し、バケットの秘匿化部分の秘匿を解除するように構成したので、古い鍵でスクランブルされたバケットと新しい鍵でスクランブルされたバケットとが受信側で混在しても符号化ビット列の復号を確実に実施できて、限定受信方式における信頼性を高めることができるという効果を奏する。

【００７４】この発明によれば、秘匿化・優先多重化制御手段が秘匿化についての優先度に基づいてバケットの秘匿特性を制御するように構成したので、各種コンテンツに応じて、あるいはコンテンツ毎の情報源符号化モードに応じて柔軟な秘匿特性を設定できるから、伝送するコンテンツの内容あるいは情報源符号化モードに応じた柔軟な秘匿機能を実現できるという効果を奏する。

【００７５】この発明によれば、秘匿化・優先多重化制御手段が秘匿化についての優先度に基づき、暗号の種類、およびＣＢＣモードやＯＦＢモード等の暗号の利用モードを変えて暗号化するように構成したので、コンテンツの内容または情報源符号化モード等に応じて秘匿の強度を適応的に制御することができるという効果を奏する。

【００７６】この発明によれば、秘匿化・優先多重化制御手段が秘匿化についての優先度に基づき、秘匿化期間を制御するように構成したので、コンテンツの内容または情報源符号化モード等に応じて、一定の期間中、契約者のみ復号可能にすること、あるいは受信者すべてに復号可能にすること等を選別して実施することができるから、受信形態を柔軟に設定することができるという効果を奏する。

【図面の簡単な説明】

【図１】　この発明の実施の形態１による限定受信方式の送信装置の構成を示すブロック図である。

【図２】　この発明の実施の形態１による限定受信方式の受信装置の構成を示すブロック図である。

【図３】　この発明の実施の形態１による限定受信方式で使用される可変長バケットの構成を示す図である。

【図４】　この発明の実施の形態１による限定受信方式における伝送信号の多重方式を説明する図である。

【図５】　この発明の実施の形態２による限定受信方式で使用される可変長バケットの構成を示す図である。

【図６】　この発明の実施の形態３による限定受信方式の送信装置の構成を示すブロック図である。

【図７】　この発明の実施の形態３による限定受信方式の受信装置の構成を示すブロック図である。

【図８】　この発明の実施の形態３による限定受信方式で使用される固定長バケットの構成を示す図である。

【図９】　この発明の実施の形態４による限定受信方式で使用される固定長バケットの構成を示す図である。

【図１０】　従来の限定受信方式の送信装置の構成を示すブロック図である。

【図１１】　従来の限定受信方式の受信装置の構成を示すブロック図である。

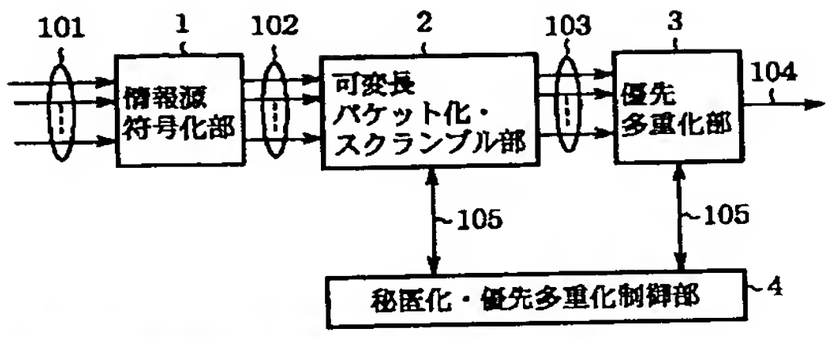
【図１２】　従来の限定受信方式における伝送信号の多重方式を説明する図である。

【符号の説明】

１　情報源符号化部（情報源符号化手段）、２　可変長バケット化・スクランブル部（バケット化・スクランブル手段）、３　優先多重化部（優先多重化手段）、４　秘匿化・優先多重化制御部（秘匿化・優先多重化制御手段）、５　優先多重分離部（優先多重分離手段）、６　可変長バケット分解・デスクランブル部（バケット分解・デスクランブル手段）、７　情報源復号部（情報源復号手段）、１０　固定長バケット化・スクランブル部（バケット化・スクランブル手段）、１１　固定長バケット分解・デスクランブル部（バケット分解・デスクランブル手段）、１０１　コンテンツ、１０２　情報源符号化ビット列、１０３　可変長バケット列（バケット列）、１０４　多重化ビット列、１０６　固定長バケット列（バケット列）、２０４　ＥＣＭ識別番号（ＥＣＭ特定番号）、２０８　ＥＣＭバージョン番号（ＥＣＭ特

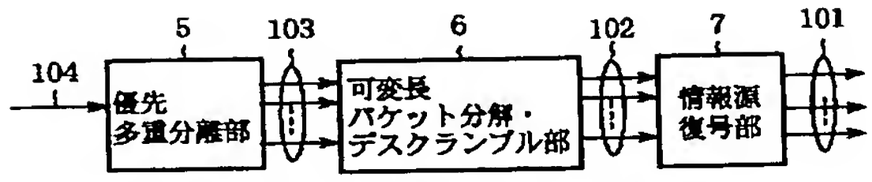
定番号）。

【図１】



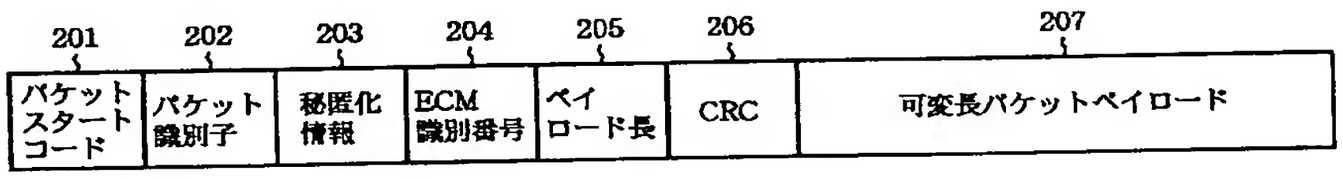
1：情報源符号化部（情報源符号化手段）
2：可変長パケット化・スクランブル部
（パケット化・スクランブル手段）
3：優先多重化部（優先多重化手段）
4：秘匿化・優先多重化制御部（秘匿化・優先多重化制御手段）
101：コンテンツ
102：情報源符号化ビット列
103：可変長パケット列（パケット列）
104：多重化ビット列

【図２】

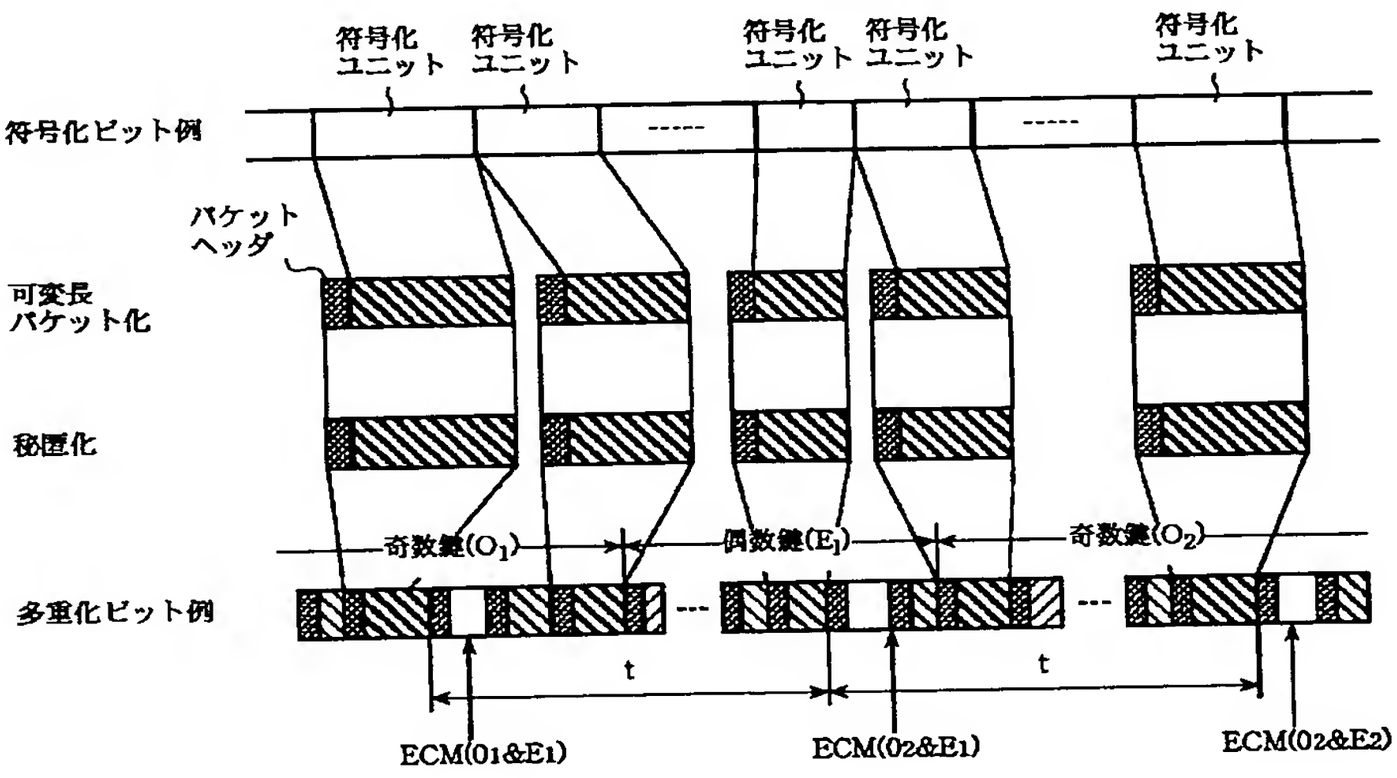


5：優先多重分離部（優先多重分離手段）
6：可変長パケット分解・デスクランブル部
（パケット分解・デスクランブル手段）
7：情報源復号部（情報源復号手段）

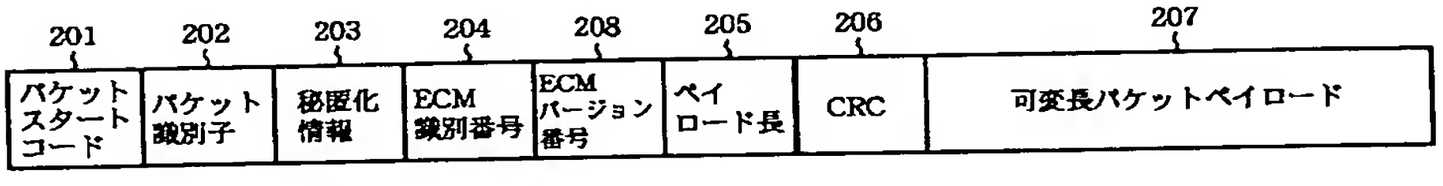
【図３】



【図４】

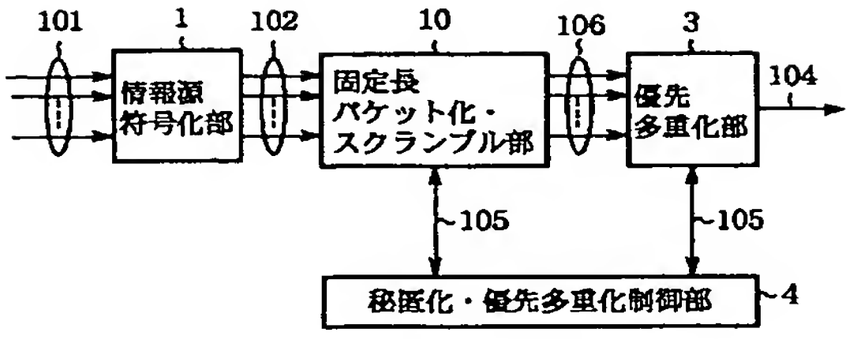


【図５】



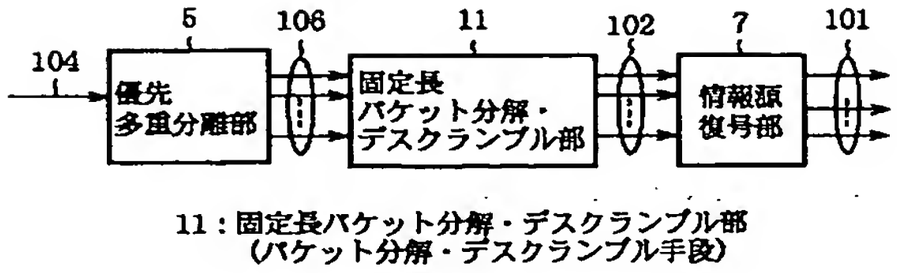
204：ECM識別番号（ECM特定番号）
208：ECMバージョン番号（ECM特定番号）

【図６】



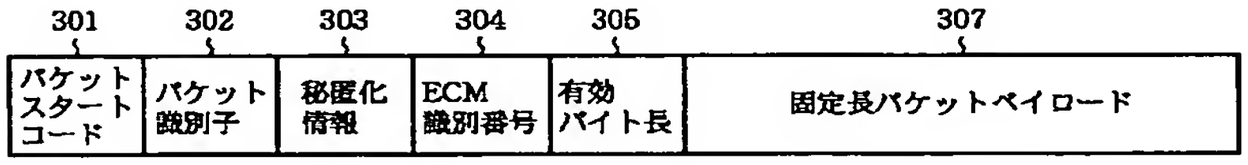
10：固定長パケット化・スクランブル部
（パケット化・スクランブル手段）
106：固定長パケット列（パケット列）

【図７】

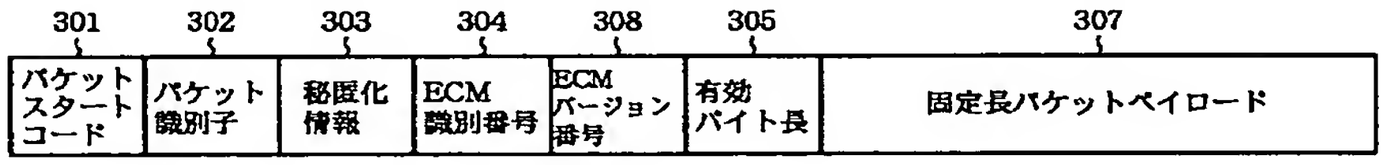


11：固定長パケット分解・デスクランブル部
（パケット分解・デスクランブル手段）

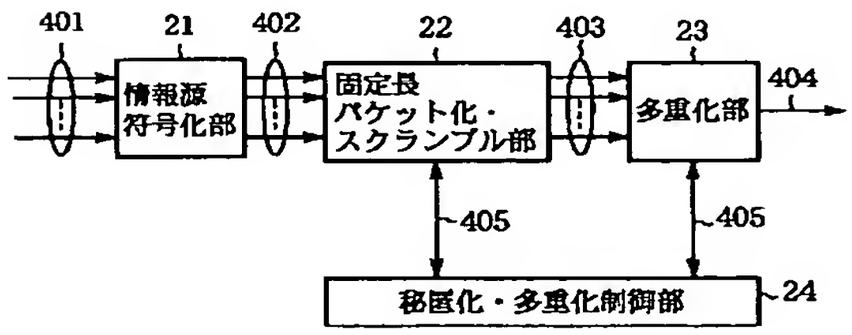
【図８】



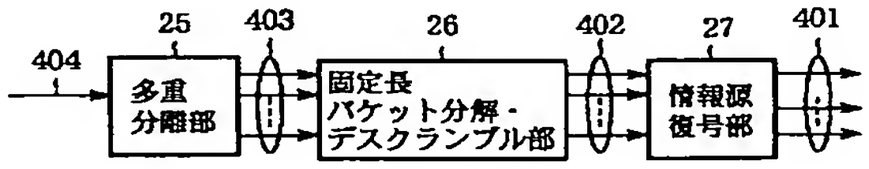
【図９】



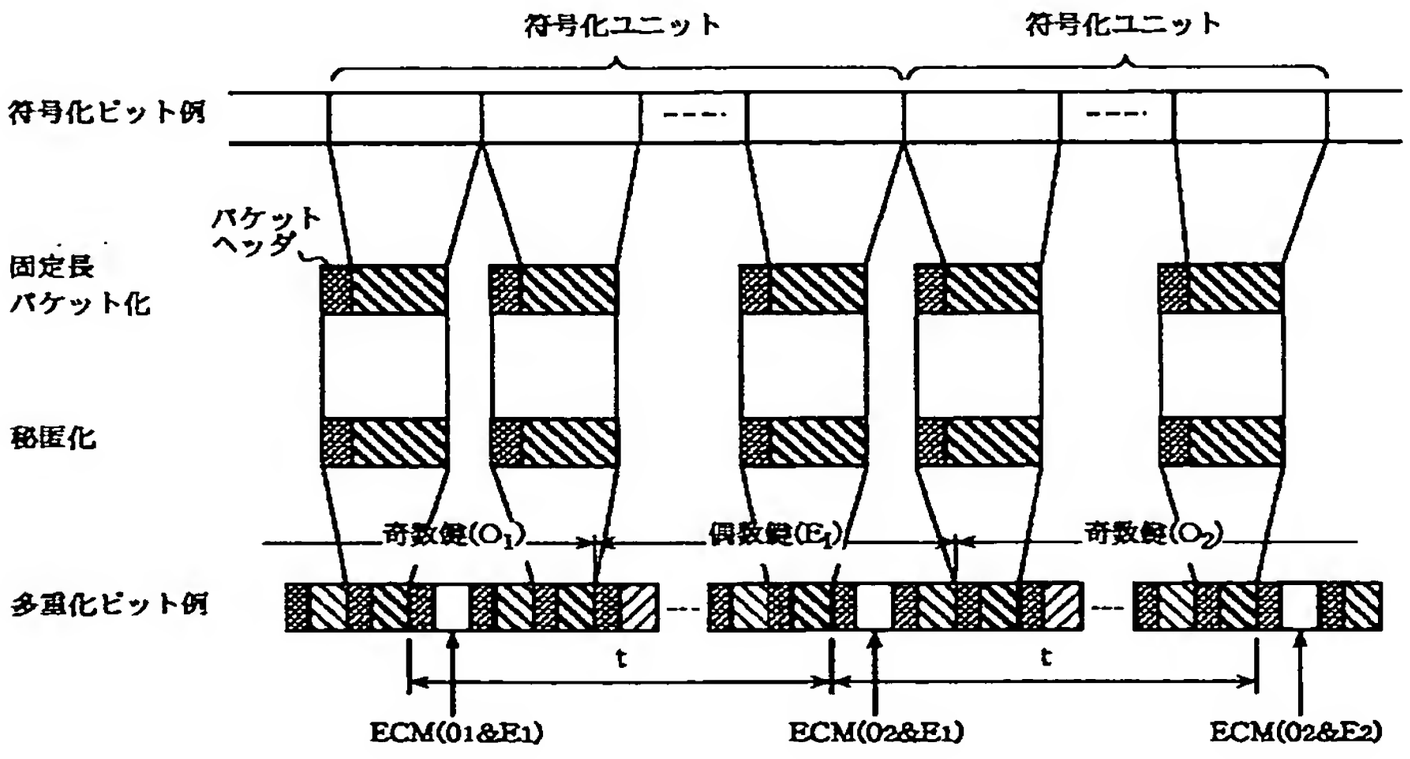
【図１０】



【図１１】



【図１２】



フロントページの続き

(51)Int.Cl.'	識別記号	F I	テーマコード（参考）
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ　7/167	Ｚ

Ｆターム(参考)　5C064 CA14 CC04
5J104 AA01 AA34 BA03 BA04 NA02
NA37 PA05
5K028 AA14 CC02 EE03 KK32 SS07
SS17 TT01
5K030 GA03 GA11 HA02 HC01 JA05
JT04 LD19

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成17年7月21日(2005.7.21)

【公開番号】特開2000-332745(P2000-332745A)
【公開日】平成12年11月30日(2000.11.30)
【出願番号】特願平11-140340
【国際特許分類第７版】
　Ｈ０４Ｌ　9/14
　Ｈ０４Ｈ　1/00
　Ｈ０４Ｊ　3/00
　Ｈ０４Ｌ　12/56
　Ｈ０４Ｎ　7/167
【ＦＩ】
　Ｈ０４Ｌ　9/00　６４１
　Ｈ０４Ｈ　1/00　Ｆ
　Ｈ０４Ｊ　3/00　Ｍ
　Ｈ０４Ｊ　3/00　Ｂ
　Ｈ０４Ｌ　11/20　１０２Ｚ
　Ｈ０４Ｎ　7/167　Ｚ

【手続補正書】
【提出日】平成16年12月1日(2004.12.1)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
　各種のコンテンツを符号化する情報源符号化手段と、
　該情報源符号化手段から出力される情報源符号化ビット列をパケットに格納するとともに該パケットの一部分を秘匿化してパケット列を生成するパケット化・スクランブル手段と、
　複数の情報源符号化ビット列をパケット単位に多重化して多重化ビット列を生成する多重化手段と、
　前記パケット化・スクランブル手段および前記多重化手段を制御する秘匿化・多重化制御手段とを有する限定受信方式の送信装置において、
　前記秘匿化・多重化制御手段が、前記多重化ビット列において、最大多重化遅延時間よりも大きな時間間隔でスクランブル鍵を更新するように制御することを特徴とする限定受信方式の送信装置。
【請求項２】
　パケット化・スクランブル手段が、情報源符号化ビット列を可変長パケットのペイロードに格納して可変長パケットを生成することを特徴とする請求項１記載の限定受信方式の送信装置。
【請求項３】
　各種のコンテンツを符号化する情報源符号化手段と、
　該情報源符号化手段から出力される情報源符号化ビット列をパケットに格納するとともに該パケットの一部分を秘匿化してパケット列を生成するパケット化・スクランブル手段と、

複数の情報源符号化ビット列をパケット単位に多重化して多重化ビット列を生成する多重化手段と、
前記パケット化・スクランブル手段および前記多重化手段を制御する秘匿化・多重化制御手段とを有する限定受信方式の送信装置において、
前記パケット化・スクランブル手段が、パケットの一部分を秘匿化するために使用したスクランブル鍵を格納するＥＣＭを特定するためのＥＣＭ特定番号をパケットのヘッダで通知することを特徴とする限定受信方式の送信装置。
【請求項４】
パケット化・スクランブル手段が、情報源符号化ビット列を可変長パケットのペイロードに格納して可変長パケットを生成することを特徴とする請求項３記載の限定受信方式の送信装置。
【請求項５】
パケット単位に多重化された多重化ビット列をコンテンツ毎のパケット列に分離する多重分離手段と、
パケット列において秘匿化された部分の秘匿を解除するとともに、パケットを分解して情報源符号化ビット列を生成するパケット分解・デスクランブル手段と、
情報源符号化ビット列を復号してコンテンツを再生する情報源復号手段とを有する限定受信方式の受信装置において、
前記パケット分解・デスクランブル手段が、ＥＣＭ特定番号を参照して、パケットの一部分を秘匿化するために使用したスクランブル鍵を特定し、パケットの秘匿化部分の秘匿を解除することを特徴とする限定受信方式の受信装置。
【請求項６】
各種のコンテンツを符号化する情報源符号化手段と、
該情報源符号化手段から出力される情報源符号化ビット列をパケットに格納して該パケットの一部分を秘匿化するパケット化・スクランブル手段と、
複数の情報源符号化ビット列をパケット単位に多重化して多重化ビット列を生成する多重化手段と、
前記パケット化・スクランブル手段および前記多重化手段を制御する秘匿化・多重化制御手段とを有する限定受信方式の送信装置において、
前記秘匿化・多重化制御手段が、秘匿化についての優先度に基づいてパケットの秘匿特性を制御することを特徴とする限定受信方式の送信装置。
【請求項７】
秘匿化・多重化制御手段は、コンテンツ毎の情報源符号化モード単位に設定された秘匿化についての優先度に基づいてパケットの秘匿特性を制御することを特徴とする請求項６記載の限定受信方式の送信装置。
【請求項８】
秘匿化・多重化制御手段は、秘匿化についての優先度に基づき、暗号の種類、およびＣＢＣモードやＯＦＢモード等の暗号の利用モードを変えて暗号化することを特徴とする請求項６または請求項７に記載の限定受信方式の送信装置。
【請求項９】
秘匿化・多重化制御手段は、秘匿化についての優先度に基づき、秘匿化期間を制御することを特徴とする請求項６または請求項７に記載の限定受信方式の送信装置。
【請求項１０】
パケット化・スクランブル手段が、情報源符号化ビット列を可変長パケットのペイロードに格納して可変長パケットを生成することを特徴とする請求項６から請求項９のいずれか１項に記載の限定受信方式の送信装置。
【請求項１１】
多重化手段は、複数の情報源符号化ビット列を該情報源符号化ビット列毎に与えられた多重化遅延に基づく優先度に基づいてパケット単位に多重化して多重化ビット列を生成することを特徴とする請求項１または請求項３または請求項６に記載の限定受信方式の送信

装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１６
【補正方法】変更
【補正の内容】
【００１６】
【課題を解決するための手段】
この発明に係る限定受信方式の送信装置は、秘匿化・多重化制御手段が多重化ビット列において、最大多重化遅延時間よりも大きな時間間隔でスクランブル鍵を更新するように制御するものである。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００１８
【補正方法】変更
【補正の内容】
【００１８】
この発明に係る限定受信方式の送信装置は、パケット化・スクランブル手段がパケットの一部分を秘匿化するために使用したスクランブル鍵を格納するＥＣＭを特定するためのＥＣＭ特定番号をパケットのヘッダで通知するようにしたものである。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００２０
【補正方法】変更
【補正の内容】
【００２０】
この発明に係る限定受信方式の送信装置は、秘匿化・多重化制御手段が秘匿化についての優先度に基づいてパケットの秘匿特性を制御するようにしたものである。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００２１
【補正方法】変更
【補正の内容】
【００２１】
この発明に係る限定受信方式の送信装置は、秘匿化・多重化制御手段がコンテンツ毎の情報源符号化モード単位に設定された秘匿化についての優先度に基づいてパケットの秘匿特性を制御するようにしたものである。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００２２
【補正方法】変更
【補正の内容】
【００２２】
この発明に係る限定受信方式の送信装置は、秘匿化・多重化制御手段が秘匿化についての優先度に基づき、暗号の種類、およびＣＢＣモードやＯＦＢモード等の暗号の利用モードを変えて暗号化するようにしたものである。
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００２３
【補正方法】変更

【補正の内容】
【００２３】
この発明に係る限定受信方式の送信装置は、秘匿化・多重化制御手段が秘匿化についての優先度に基づき秘匿化期間を制御するようにしたものである。
この発明に係る限定受信方式の送信装置は、多重化手段が、複数の情報源符号化ビット列を該情報源符号化ビット列毎に与えられた多重化遅延に基づく優先度に基づいてパケット単位に多重化して多重化ビット列を生成するようにしたものである。
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００７０
【補正方法】変更
【補正の内容】
【００７０】
【発明の効果】
以上のように、この発明によれば、秘匿化・多重化制御手段が多重化ビット列において最大多重化遅延時間よりも大きな時間間隔でスクランブル鍵を更新するように制御する構成としたので、受信側において古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが混在するのが防止されるから、符号化ビット列の復号を確実に実施できて、限定受信方式における信頼性を高めることができるという効果を奏する。
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００７２
【補正方法】変更
【補正の内容】
【００７２】
この発明によれば、パケット化・スクランブル手段がパケットの一部分を秘匿化するために使用したスクランブル鍵を格納するＥＣＭを特定するためのＥＣＭ特定番号をパケットのヘッダで通知するように構成したので、当該パケットのスクランブル処理に使用されたスクランブル鍵を特定することができるから、古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが受信側で混在しても符号化ビット列の復号を確実に実施できて、限定受信方式における信頼性を高めることができるという効果を奏する。
【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００７４
【補正方法】変更
【補正の内容】
【００７４】
この発明によれば、秘匿化・多重化制御手段が秘匿化についての優先度に基づいてパケットの秘匿特性を制御するように構成したので、各種コンテンツに応じて、あるいはコンテンツ毎の情報源符号化モードに応じて柔軟な秘匿特性を設定できるから、伝送するコンテンツの内容あるいは情報源符号化モードに応じた柔軟な秘匿機能を実現できるという効果を奏する。
【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００７５
【補正方法】変更
【補正の内容】
【００７５】
この発明によれば、秘匿化・多重化制御手段が秘匿化についての優先度に基づき、暗号

の種類、およびＣＢＣモードやＯＦＢモード等の暗号の利用モードを変えて暗号化するように構成したので、コンテンツの内容または情報源符号化モード等に応じて秘匿の強度を適応的に制御することができるという効果を奏する。

【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】００７６
【補正方法】変更
【補正の内容】
【００７６】

この発明によれば、秘匿化・多重化制御手段が秘匿化についての優先度に基づき、秘匿化期間を制御するように構成したので、コンテンツの内容または情報源符号化モード等に応じて、一定の期間中、契約者のみ復号可能にすること、あるいは受信者すべてに復号可能にすること等を選別して実施することができるから、受信形態を柔軟に設定することができるという効果を奏する。